HN

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/698,159	10/30/2000	Anup K. Ghosh	CIG-103	7526

7590 01/12/2005

Brett C. Martin
1650 Tyson Blvd.
McLean, VA 22102

EXAMINER	
TRAN, ELLEN C	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 01/12/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Offic Action Summary	**Application N .** 09/698,159	**Applicant(s)** GHOSH ET AL.	
	Examiner Ellen C Tran	**Art Unit** 2134	

-- The MAILING DATE of this communication appears n the cover sheet with the correspondence address --

Period f r Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 June 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8,12-19,23-30,33-44 and 47-50* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8,12-19,23-30,33-44 and 47-50* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)	4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)	5) ☐ Notice of Informal Patent Application (PTO-152)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.	6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to communication: 7 June 2004, the original application was filed on 30 October 2000 with a continuing application priority date of 28 October 1999.

2. Claims 1-8, 12-19, 23-30, 33-44, 47-50 are currently pending in this application. Claims 1, 12, 23, and 37 are independent claims. Claims 9-11, 20-22, 31, 32, 45, and 46 have been cancelled. Claims 3, 4, 14, 15, 25, 26, 39, and 40 have been amended.

3. Due to amendment claim objections, 112 rejections, and 101 rejections are withdrawn.

Response to Arguments

4. Applicant's arguments with respect to claims 1-8, 12-19, 23-30, 33-44, 47-50 have been considered but are not persuasive.

In response to argument starting on page 15 line 3, **"The system described in Munson utilizes multinomial distributions to determine abnormality. The present system employs neural networks that have been previously trained to identify normal behavior"** the Office disagrees with this argument. Reference '331 does teach system training to identify intrusions, see col. 14, line 41 through col. 15, line 15 "In the absence of these specifications, it will be assumed that neither the operational profiles nor the functional profiles can be observed directly. Instead, the distribution of activity among the program modules must be observed in order to make inferences about the behavior of the system. The present invention, then, represents a new real-time approach to detect aberrant modes of system behaviors induced by abnormal and unauthorized system activities ... In contrast, the present invention operates in real time, from within the application being monitored and is able to respond to subtle changes that occur as a result of an intrusion". The reference teaches observing the activities of the system while executing software and then updating the profile to account for behavior. This method utilizes observations to identify intrusion. The observed activities, which are monitored and compared is the same process as training a system to identify abnormalities.

In response to argument starting on page 15, line 16, **"Regarding the rejection with respect to claims 1 and 12 ...a) of each claims 1 and 12 is not supported by the cited passage. Element a) specifically recites "each said first application profile comprises a plurality of first data strings, wherein each first data string comprises a sequential mapping of instructions"**. The Office disagrees the cited passage "During the software design process, the basic functions are mapped by a system designers to specific software program modules that implement the functionality" in combination with the complete reference '331 shows how these basic functions are used to establish a profile which is updated based on the observed behavior, see '331 col. 7, lines 61 through col. 8, line 47 "The design process may be thought of as the process of defining a set of relations ... Each operation that a system may perform for a user may be thought of as having been implemented in a set of functional specifications". The "functional specifications" has the same meaning as "sequential mapping of instructions".

In response to argument starting on page 16, **"Regarding the "second application profiles" allegedly describe in Munson at co. 9, lines 49-55, this passage discusses that each user may have a unique characteristic operational profile ... Munson does not describe any relation between the characteristic operational profile and any other profile in the cited portion of column 4"**. The Office disagrees with the argument the brevity shown in the Office Action should not prevent the applicant from seeing how the references teaches that initial profiles are established and that they are monitored and updated over time based on observed behavior see '331 col. 8, lines 38-58 and col. 9, lines 49-66 "Each user may potentially bring his/her own distinct behavior to the system ... Thus each user will have a unique characteristic operational profile. It is a characteristic, then of each user to induce a probability function ... As the system progresses through the steps in the software lifecycle, the user requirements specification, the set O must be mapped on a specific set of functionalities F by system designers. This set F is in fact the design specifications for the system ... Thus, a new indexed collection of random variables $\{Y_t\}$ may be defined, representing the individual transitions events among particular functionalities".

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language

6. **Claims 1, 2, 5, 7, 8, 12, 13, 16, 18, 19, 23, 24, 27, 29, 30, 37, 38, 41, 43, and 44** are rejected under 35 U.S.C. 102(e) as being anticipated by Munson et al. U.S. Patent No. 6,681,331 (hereinafter '331).

As to independent claim 12, "A method for detecting intrusive behavior" is taught in '331 col. 2, lines 10-11;

"in a first session on a computer, said first session comprising a plurality of applications invoked on said computer, and said computer having a computer operating system, said method comprising the steps of:" is shown in '331 col. 6, lines 30-34;

"(a) creating a plurality of first application profiles, wherein each said first application profile comprises a plurality of first data strings, wherein each first data string comprises a sequential mapping of instructions passed from one of said plurality of applications to the computer operating system during a second session on the computer" is disclosed in '331 col. 7, lines 17-20;

"(b) creating a plurality of second application profiles, wherein each second application profile comprises a plurality of application segments, wherein each application segment comprises a pre-determined number of second data strings, wherein each second data string comprises a sequential mapping of instructions passed from one of said applications to the computer operating system during the first session on the computer" is taught in '331 col. 9,

lines 49-55;

"(c) initializing an application counter;

(d) initializing a plurality of segment counters, wherein each segment counter corresponds to one of the second application profiles" is shown in '331 col. 8, lines 16-37;

"(e) initializing a plurality of data string counters, wherein each data string counter corresponds to one of the application segments in the plurality of application segments" is disclosed in '331 col. 13, lines 2-3 and col. 14, lines 25-26;

"(f) performing an equality matching algorithm, wherein for each application segment, each second data string is compared to the plurality of first data strings comprising a corresponding application profile, and wherein if the second data string is not equal to any of the first data strings an associated data string counter is incremented; and

(g) performing a temporal locality identifying, algorithm, wherein the first session is labeled intrusive if a ratio of the segment counter to a total number of segments in an associated second application profile exceeds an application threshold and wherein the first session is labeled intrusive if a ratio of the application counter to a total number of applications exceeds a session threshold, wherein the application counter is incremented if a ratio of an associated segment counter to a total number of segments in an associated second application profile exceeds a segment threshold, wherein the associated segment counter is incremented if a ratio of an associated data string counter to the pre-determined number of data strings comprising the segment exceeds an associated data string threshold" is taught in '331 col. 4, lines 26-65.

As to dependent claim 13, "wherein the second session comprises non-intrusive behavior" is shown in '331 col. 4, lines 30-33.

As to dependent claim 16, "herein the first plurality of application profiles and second plurality of application profiles are created by a data pre—processor application" is disclosed in '331 col. 4, lines 33-40.

As to dependent claim 18, "wherein the data pre-processor creates the second plurality of application profiles in real-time" is taught in '331 col. 6,

lines 11-12

As to dependent claim 19, "wherein the equality matching algorithm and the temporal locality identifying algorithm receive input from the second plurality of application profiles in real-time" is shown in '331 col. 6, lines 11-15.

As to independent claim 1, this claims is directed to the detection system of the method of claim 12 and is similarly rejected along the same rationale.

As to dependent claims 2, 5, 7, and 8, these claims incorporate substantially similar subject matter as in cited in claims 13, 16, 18, and 19 above and are rejected along the same rationale.

As to independent claim 37, "A method for detecting intrusive behavior" is taught in '331 col. 2, lines 10-11;

"in a session on a computer, said session comprising a plurality of applications invoked on said computer, and said computer having a computer operating system, said method comprising the steps of" is shown in '331 col. 6, lines 30-34;

"(a) training a plurality of neural networks, wherein each neural network is trained to identify a pre-determined behavior pattern for a corresponding one of the plurality of applications" is disclosed in '331 col. 7, lines 17-20;

"(b) creating a plurality of application profiles, wherein each application profile comprises a plurality of application data for a corresponding one of the plurality of applications, wherein said application data is collected during the session" is taught in '331 col. 9, lines 49-55;

"(c) performing a temporal locality identifying algorithm, wherein when one of the plurality of application profiles is sequentially input to a corresponding one of the plurality

of neural networks the neural network outputs a behavior indicator for each of the plurality of data strings in the application profile, and wherein if the behavior indicator meets a pre-determined criteria, a counter is incremented, and wherein if the counter has a high rate of increase the temporal locality identifier labels the application behavior intrusive, and wherein if a predetermined percentage of application behaviors are intrusive the session behavior is labeled intrusive" is taught in '331 col. 4, lines 26-65.

As to dependent claims 38, 41, 43, and 44 these claims incorporate substantially similar subject matter as in cited in claims 13, 16, 18, and 19 above and are rejected along the same rationale.

As to independent claim 23, this claim is directed to the detection system of the method of claim 37 and is similarly rejected along the same rationale.

As to dependent claims 24, 27, 29, and 30 these claims incorporate substantially similar subject matter as in cited in claims 13, 16, 18, and 19 above and are rejected along the same rationale.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. **Claims 3, 4, 6, 14, 15, 17, 25, 26, 28, 39, 40, and 42,** are rejected under 35 U.S.C. 103(a) as being unpatentable over '331 in further view of Rowland U.S. Patent No. 6,405,318 (hereinafter '318).

As to dependent claim 17 the following is not taught in '331 **"wherein the data pre-processor receives input from an auditing system integral to the computer operating system"** however '318 teaches "The system combines the above listed capabilities with real-time monitoring of log audit files, port scan detection capability and session monitoring" in col. 2, lines 65-68.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the intrusion detection system taught in '331 to include a means to utilize audit reports to improve intrusion detection. One of ordinary skill in the art would have been motivated to perform such a modification to automatically build user profiles see '318 (col. 2, lines 40 et seq.) "The present invention provides a real-time intrusion detection method and system. The intrusion detection system automatically and dynamically builds user profile data".

As to dependent claim 14 "wherein and the sequential mapping of instructions comprise a sequential mapping of system calls" is taught in '318 col. 4, lines 34-40 "for a Unix® based operating system or may be event logs for a Windows NT® operating system. The system checks to determine if the user should be ignored".

As to dependent claim 15 "wherein the sequential mapping, of instructions comprises a sequential mapping of object requests" is shown in '318 col. 4, lines 34-40 "for a Unix® based operating system or may be event logs for a Windows NT® operating system. The system checks to determine if the user should be ignored".

As to dependent claims 3, 4, and 6, these claims incorporate substantially similar subject matter as in cited in claims 14, 15, and 17; therefore they are rejected along the same rationale.

As to dependent claims 25, 26, and 28, these claims incorporate substantially similar subject matter as in cited in claims 14, 15, and 17; therefore they are rejected along the same rationale.

As to dependent claims 39, 40, 42, 45, and 46 these claims incorporate substantially similar subject matter as in cited in claims 14, 15, 17; therefore they are rejected along the same rationale.

9. **Claims 33-36 and 47-50** are rejected under 35 U.S.C. 103(a) as being unpatentable over '331 in further view of Bergman et al. U.S. Patent No. 6,442,694 (hereinafter '694).

As to dependent claim 47, the following is not taught in '331 **"wherein the plurality neural network comprises a plurality of backpropogation neural networks"** however '694 teaches "In describing the processing which take place at a particular nodes, it is useful to define some terms related to the timing of such processing. Time delays for processing an d transmission of messages at each of nodes 42 are denoted as follows:" in col. 11, lines 50-67.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the intrusion detection system taught in '331 to include a means to examine the backpropogation of the network. One of ordinary skill in the art would have been motivated to perform such a modification to improve intrusion detection system see '694 (col. 5, lines 9 et seq.) "In view of the above, it has been recognized that since the results of component failures and attacks are often similar (e.g. improper operation of one or more network components or nodes), the difference is transparent ot a network nor or system user. Because of this transparency there is no absolute metric to determined whether an input is fault or not".

As to dependent claim 48, "herein each neural network in the plurality of backpropogation neural networks comprises an input layer, a hidden layer and an output layer" is taught in '694 col. 15, lines 19-26 "From the above processing steps it can be seen that no node will generate an alarm until at least one attack is detected. When an attack occurs only the first node experiencing the attack will respond with an alarm. All nodes downstream from the first node receive messages which indicate that the node upstream experienced an attack".

As to dependent claim 49, "wherein a number of nodes in the hidden layer is determined by testing a plurality of cases for each neural network in the plurality of backpropogation neural networks and selecting the case wherein the corresponding neural network has a highest accuracy rate" is shown in '694 col. 6, lines 35-48 "The test on a unit to determine whether it is faulty or operational is reliable only for operational units. Necessary and sufficient conditions for the testing structure for establishing each unit as faulty or operational as long as the total number of faulty elements is under some bound are known".

As to dependent claim 50, "wherein the plurality of neural networks comprises a plurality of recurrent neural networks" is disclosed in '694 col. 10, lines 9-21 "It should be noted that the techniques of the present invention have applicability to a wide variety of different types of networks and is advantageously used in theses application".

As to dependent claims 33-36 these claims incorporate substantially similar subject matter as in cited in claims 47-50 above and are rejected along the same rationale.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a). A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 6:30 am to 3:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A Morse can be reached on (571) 272-3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ellen Tran
Patent Examiner
Technology Center 2134
04 January 2005

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100